**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 285**

Security Equipment

**Security hardware**

1. What is meant by data integrity?

Data integrity is the assurance that data is accurate, reliable, and hence timely supplied.

1. Biometrics
   1. Describe biometric security.

Biometric security is the use of physical human characteristics, including finger prints or behavioural characteristics such as voice or handwriting to grant a user access to a resource/area.

* 1. Why does it appeal to security managers?

Its appeal comes from the near impossibility of unauthorised personell copying or stealing to gain access.

* 1. List the common biometric devices.

Common biometric devices include;

* Voice recognition or comparing a person’s speech with a stored voice pattern. For this a user must record several words multiple times so patterns can be found.
* Fingerprint recognition works by detecting each small ridge and swirl of a fingerprint at normally a resolution of 800 dpi and then attempting to match at least 20 points against pre-scanned image of a user’s fingerprint.
* Hand geometry which measures the size and layout of the hand as well as any key features noted. This is the predecessor of fingerprint technology.
* Signature verification which compares the signatures key information (pressure, motion and location) that you have just written on a pressure sensitive tablet to one stored.
* Facial recognition which recognises 80 points on the human face such as distance between the eyes, chin line and depth of eyes to name but a few. It can distinguish users in front or moving within the crowd and is often used by authorities.
* Iris recognition works on using one of the most unique features of a person, their iris. For this reason it is believed to be the most accurate methods available and as such it checks up to 247 independent points on the iris. Due to their high expense they are often only used for military or financial institutions sensitive data.
  1. What are the concerns of biometric technology?

The key concern of biometric technology originates from the potential intrusiveness of the technology, similarly the cost of such technology can also hold back the acceptance of the technology.

1. Swipe cards
   1. Describe the nature of a swipe card.

Swipe cards are a common type of security device used by many people usually plastic with a magnetic strip. Common examples include ATM cards or other information accessing cards such as loyalty cards. They are now common methods accessing areas restricted in access.

* 1. What is a limitation of the swipe card?

A swipe card suffers from the fact that it can easily be damaged or stolen physically or via a swipe card reader digitally.

1. Smart cards

Smart cards are a recent advance in card technology, looking much like a swipe card it however differs due to the inclusion of a microchip embedded to store and manipulate data. For example it may commonly be used prepaid telephone cards or the recent myki ticketing system. They will commonly store 2kB to 10MB of memory.

1. Security tokens

Security tokens are commonly used when dealing with sensitive data and is a small device about the size of a keyring displaying a constantly changing authentication code. By entering the account name and the password a security token will now display a authentication code that can be used to access the relevant information. This is a example of a two factor authentication code meaning that losing the device will not guarantee the thief access unless the username and password is also known.

1. Mobile phone secure code
   1. How does this level of authentication work?

A mobile secure code is a variant of the security token in that it provides another layer of protection on the simple username/password as a authentication code is sent to the users phone to confirm identity before proceeding to the account or a certain action.

**Power protection**

Outline the characteristics of the following:

1. Surge protector

A surge protector protects electrical equipment against overvoltage from a power surge by smoothing the current. It is worth noting that it may be damaged overtime or through protecting from a severe surge and as such should be replaced occasionally.

1. Uninterruptible power supply, (UPS)

A UPS is simply a high quality surge protector with a inbuilt battery to help supply a constant current while also supplying power directly following a power outage for a determined time to allow users to hurry and save then turn off the device ensuring data isn’t lost nor the hardware damaged.

**Strategies for avoiding system failure, p 288**

1. What is meant by redundancy?

Redundancy is the building in of an extra item that isn’t necessary for something to function however it assist preventing some issues. Ie a backup helps prevent data loss on one device being irreversible or an error that will stop work.

1. What is meant be a fault-tolerant server?

Fault tolerant servers are servers that will continue to work even after a piece of hardware has failed. This is achieved by implementing a redundant item such as a having dual hard drives, motherboards, power transformers ect running in parallel so that a failure of one will not cause issues, similarly maintenance can be conducted without interrupting basic operations.

1. Redundancy through multiple hard drives or fault-tolerant equipment
   1. Describe how this redundancy works.

This type of redundancy works by ensuring that there is always a backup methods such as a mirrored hard drive to prevent the issue.

* 1. What is meant by RAID technology

RAID or Redundant Array of Inexpensive Disks refers to when data fragments are spread out across the several disks ensuring that the data can be reconstructed if the one disk fails using error checking codes.

1. Redundancy through mirrored servers or machines
   1. Why is the RAID solution preferable to this solution?

RAID is preferable to mirrored servers or machines due to the potential lower costs involved.

**Backup Media**

1. There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?

When deciding on the type of backup media to use you should consider;

* Cost of the drive and required media
* Speed achievable
* Compatibility both current and for the future, ie if you are using XP data then it has to be compatible however you should also ensure that you will be able to use it for a decent time frame in the future as well.

Three categories of backup media:

* Magnetic
* Optical
* Solid state

List the characteristics of the following backup media:

**Magnetic media**

1. hard disk drive

An affordable option may include backing up to a second internal hard disk, especially if you have many files. However the use of external is useful in the event of a disaster such as flood or fire.

1. Magnetic tapes

Magnetic tapes are very popular form of media for backup files due to their relative cheapness, this however comes at a sacrifice to speed with this method of backup requiring sequential access.

**Optical media**

1. Compact disc

Compact discs are removable storage media that can hold up to 700 MB of data (approx.. 80 min of audio). The may be either CD-R (A write once, read many), CD-RW (right and read many like a usb), CD+R (write many ready many like a printed file) ect.

1. DVD

A DVD (Digital Versatile Disk) is a growingly preferred backup medium with high amount of data being able to be recorded to it (upto 17 GB if double sided). Like CD-ROMs they come in a few varients such as DVD-R that can be recorded once or DVD-RW which can be recorded many times.

1. Blu-ray

Blu-ray is a optical disk format with a capacity of up 50 GB if dual layer and designed to replace DVDs. The name comes from the blue laser used to read the disk allowing for 5x more data to be stred as well as consequentally HD films or other digital media.

**Solid-state drives**

1. USB storage devices

A USB (Universal Serial Bus) are popular method of backing up both large and small amounts of data, similarly their small size makes then a preferred method of storing data portably. As there is no moving parts due it being solid state it also has less chance of failure. USBs have been steadily increasing in there storage size though a common maximum size is 256 GB. Likewise they come in a wide variety of size and shapes.

**Online backups**

1. Why do organisations use this form of backup?

Organisation use this form of backup as they offer a form of offsite storage, with a high fault tolerance through use of redundancy, UPS’s ect.

1. Describe an enterprise storage system.

A enterprise storage system typically involves the interconnection via a storage area network (SAN), or RAID disks, tapes, CD/DVD-ROM servers, internet backup and other networked attached devices.

**Surveillance technology, p 292**

Describe the nature of the following items of surveillance equipment used in offices:

1. Packet sniffers

Packet sniffers use diagnostic tools to monitor the contents of packets of data being sent across the network. They can also filter packets containing certain data elements and copy them to a admin computer for further analysis. They are commonly used to ensure that appropriate use of email and internet usage.

1. Desktop monitoring programs

Desktop monitoring programs work by intercepting every single action preformed on the computer. This type may be used by either admins or hackers ect. This data is generally recorded to a log file for feature reference and may include screen dumps

.

1. Log files

Log files are recorded can be recorded by a program that is dedicated to that purpose or not. For example a web server will log who, what looked at and how long, Windows will record events ect

1. Closed-circuit television, (CCTV)

CCTV is used to monitor the happenings in the workplace itself. The cameras may either be concealed or plain view to discourage.

1. Telephones

Phone tapping may occur to ensure that the reasource is only being used for work purposes. A example of this is when call centres inform you that the call may be recorded.

1. Audit trails

Audit trails are the recording of each time that information is altered or transferred so that if a problem arises they can be traced back to the source.

**Physical security devices:** List the options for physically securing your data

To physically secure you data you may;

* Use lock-box’s, safes and the likes
* Locked rooms
* Security cables
* Locked Cases or docks
* Daisy chained or padlocked cables